UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/082,982	02/25/2002	Chaing Chen		1878

7590 07/19/2005

CHAING CHEN
8778 BOULDER RIDGE RD
LAUREL, MD 20723-5901

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/082,982	CHEN ET AL.	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *(1) 5/22/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the application filed on 2/25/2002.

2. Claims 1-20 are under examination.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 6, 8-11, 14, 15 18, 19 and 20 are rejected under 35 USC 103 (a) for being unpatentable over Yu et al (US Patent No. 6,067,621) in view of Vaeth et al (US Patent No. 6,035,402), and further in view of Brown et al (US Patent No. 6,658,415, M. Brown).

As per claim 1, Yu teaches:

(a) authentication authority means to serve as a powerhouse to authenticate user identity **[Yu, *col. 6 lines 12-14*, "a server 140 for authenticating the one-time password generated from the transaction terminal 120 (i.e. user) to provide transaction services"]**,

(c) authentication client means to serve as an end-user device to generate said one-time identity codes **[Yu *col. 6 lines 6-10* "The user authentication system includes**

an IC card 100 for safely keeping and carrying personal secret information, a transaction terminal 120 which is miniature and portable for generating a one-time password to confirm the identity of a person"],

(e) i. transmitting said one-time identity codes from said authentication client means to said authentication handler means **[Yu, *col. 9 lines 27-34* "The portable terminal 120 submits the card access key received during the initialize service of the IC card 100, reads the secret values (a secret key for a symmetrical cipher algorithm) in the IC card 100, and generates the one-time password at step 430. When the user transfers this result to the server 140 at step 440, the server 140 verifies the one-time password received from the portable terminal 120 at step 450"],**

whereby the authentication system can be used as an ID verification system for said business entities to verify said user identity over a channel selected from the group consisting of the Internet, phone and other communication means **[Yu, *col. 3 lines 55-59* "a password receiver for receiving the one-time password generated in the terminal through a telephone line or a network, and a password verifier for verifying whether the received password is identical to the generated password"],**

Vaeth teaches:

(b) gateway authority means to serve as a gateway to delegate said authentication authority Web services to said authentication authority means **[Vaeth *col. 6 lines 49-53* "the CA may generate and host an Internet (or Intranet) web site on behalf of multiple RAs or have certificate requests to an RA-maintained web site linked**

invisibly to the CA to provide a "virtual CA" " Fig. 3 (i.e. CA delegates authority (or responsibility) to RA)],

(e) ii. composing authentication requests by said authentication handler means, and transmitting said authentication requests from said authentication handler means to means selected from the group consisting of said gateway authority means and said authentication authority means **[Vaeth *col. 6 lines 7-13* "requesters** (authentication handler) **(a) requesting certification on a network from a "web site" (like the "World Wide Web" of logically linked Internet nodes) of the CA** (gateway authority) **reached with a network browser, and (b) providing information including verification or qualification data and the requester's public key; (2) the RA** (authentication authority) **(a) accessing the certificate request information via the network]**,

iii. processing said authentication requests by said gateway authority means, and redirecting said authentication requests from said gateway authority means to said authentication authority means **[Vaeth, Fig. 3** CA(gateway authority) and RA(authentication authority) communicate using communication link 175, 195, 185, 187 Therefore GA redirect the request to AA, ***col. 6 lines 15-19* "the CA (a) generating the certificate with the requester's public key and the public key of the certificate authority, (b) signing the certificate using the private key of the certificate authority; and (c) delivering the certificate to the requester on the network col. 6 lines 12-13 the RA (b) approving the request, and (c) sending the approval to the CA via the network"]**,

iv. generating authentication responses by said authentication authority means, and transmitting said authentication responses back to said authentication handler means, whereby a scalable and distributable system to authenticate and validate said user identity will be provided **[Vaeth, *col. 6 line 14* "sending the approval to the CA via the network",** RA and requester communicate using communication link 185,175 **]**,

M. Brown teaches:

(d) authentication handler means to serve as a doorkeeper to protect resources of business entities using said authentication authority Web services **[Brown, *col. 6 lines 17-19, 20-27, 34-35, 57-63* Fig. 3A "a server system 80 is advantageously an authority-enabled platform that supports electronic business for a particular retailer or consumer provider. Accountability application 98 compares the product requested for purchase by the user with the authority-designated products and services and controls an access signal to check-point device 134 indicating whether or not the user is allowed access to purchase the particular book according to the authority-designated settings"].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Vaeth and M. Brown into the teaching of Yu to utilize CA (i.e. gateway authority) to delegate authority to RA (i.e. authentication authority) and to use authentication handler for serving as a doorkeeper to protect the resource.

The modification would be obvious because one of ordinary skill in the art would be motivated to (i) direct the requests for a certificate, along with verification

information to the certificate authority, where they are held and accessed by an entity having verification responsibilities (RA) and approved and disapproved. So that the network linking providing flexibility functionality minimized RA investment and allows the CA to concentrate on providing security at the most security-sensitive portion of the system **[Vaeth, *col. 6 lines 53-57*]** and (ii) monitor and manage user access to content. The particular user is only allowed access to a selection of multiple of types of content from the authority-enabled system that are enabled according to the authority-designated setting received via network according to particular universal identifier associated with a particular user **[M. Brown, *col. 2 lines 23, 34-40*]**.

As per claim 6, the rejection of claim 1 is incorporated and further Vaeth teaches:

said gateway authority means and said authentication authority means contain means to be separated and placed in the Internet accessible environment to become said scalable and distributable system **[Fig. 3 CA** (i.e. gateway authority) **and RA** (authentication authority) **are separate authority and they are placed in the Internet accessible environment]**.

As per claim 8, the rejection of claim 1 is incorporated and further Yu teaches:

authentication authority means contain means for independently generating said one-time identity codes to authenticate said user identity **[Fig. 3 *col. 7 lines 40-43* "The**

second password generator 144 is installed to read the secret key and the random number stored in the secret key memory 141, and generate the one-time password by the same predetermined method used in the terminal 120"].

As per claim 9, the rejection of claim 1 is incorporated and further Vaeth teaches:

authentication authority means contain means to use platforms which are vendor independent **[*col. 9 lines 32-36* "the platforms used for the servers, router and firewall are designed so that additional capacity or devices can be added with little impact to the hardware and/or software in the on-line portion of CA facility 190"].**

As per claim 10, the rejection of claim 1 is incorporated and further Vaeth teaches:

said authentication responses generated by said authentication authority means contain means to inform said authentication handler said user identity **[*col. 8 lines 35-38* "In verification step 409, which may be performed on a batch basis, RA 180 compares the CRD data with the data in its registration database 189 and approves or disapproves the certificate request"** (RA and Requester communicate using communication link 175,185)**].**

As per claim 11, the rejection of claim 1 is incorporated and further Yu teaches:

authentication authority means and said authentication client means contain means to generate synchronization codes (i.e. single-use password) and conduct synchronization **[*col. 8 lines 12-17* "The counter memory 145 stores a counter value for synchronizing the terminal 120 with the server 140. The counter changer 146 changes the counter value into a predetermined value and stores the same in the counter memory 145 whenever a single one-time password is generated", Fig. 2, 3].**

As per claim 14, the rejection of claim 11 is incorporated and further Yu teaches:

said authentication authority means and said authentication client means contain means to generate confirmation codes to verify the success of said synchronization **[*col.6 lines 10-11* "a transaction terminal 120 which is miniature and portable for generating a one-time password to confirm the identity of a person", *col. 11 lines 50-54* "If the process for confirming the password remembered by only the user is added to the user authentication process of the user authentication system according to the principles of the present invention, a safer user authentication is available"].**

As per claim 15, the rejection of claim 1 is incorporated and further Yu teaches:

said authentication authority means and said authentication client means contain means to independently generate non-predictable sequence number (i.e. random number) which is an essential part for producing said one-time identity codes **[Fig. 2 and Fig. 3].**

As per claim 18, the rejection of claim 1 is incorporated and further Yu teaches:

authentication client means contain means to be incorporated in a portable, hand-held device **[*col. 6 lines 8-9* "a transaction terminal 120 which is miniature and portable for generating a one-time password"].**

As per claim 19, the rejection of claim 1 is incorporated and further M. Brown teaches:

authentication handler means (i.e. accountability application 98) is arranged to be executed on said business entities' computers (i.e. server system 80) **[Fig. 3A].**

As per claim 20, the rejection of claim 1 is incorporated and further M. Brown teaches:

authentication handler means (i.e. accountability application) contain means to receive and process said user logon request, compose and submit authentication request to said authentication authority means, process and validate returned authentication

response from said authentication authority means, and grant permission for said user to log onto said business entities' computer **[*col. 6 lines 57-63* "Accountability application 98 compares the product requested for purchase by the user with the authority-designated products and services and controls an access signal to check-point device 134 indicating whether or not the user is allowed access to purchase the particular book according to the authority-designated settings"].**

4. Claims 2, 3, 4 and 5 are rejected under 35 USC 103 (a) for being unpatentable over Yu et al (US Patent No. 6,067,621) in view of Vaeth et al (US Patent No. 6,035,402), in view of Brown et al (US Patent No. 6,658,415, M. Brown) and further in view of Brown et al (US Pub No. 2002/0169988, L. Brown).

As per claim 2, the rejection of claim 1 is incorporated and L. Brown teaches:

gateway authority means contain means to interact with other entities of said gateway authority means, and publish said authentication authority Web services to Web service industry's registries **[*page 2 paragraph 0025*, Fig. 1 "Service providers 11 host a network accessible software module. A service provider defines a service description for a Web service and publishes it to a service registry 13"].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of L. Brown into the teaching of Yu, Vaeth and M. Brown that use Web services to publish and discover the

information. The modification would be obvious because one of ordinary skill in the art would be motivated to use Web services because Web services offers the dual promise of simplicity and pervasiveness. Web services are based on the extensible Markup Language (XML) standard data format and data exchange mechanisms, which provide both flexibility and platform independence **[L. Brown, *page 1 paragraph 0002, 0006*].**

As per claim 3, the rejection of claim 2 is incorporated and further L. Brown teaches:

gateway authority means are arranged to use Web Services Description Language (WSDL) to publish said authentication authority Web services, and use Universal Description, Discovery and Integration (UDDI) standard to discover said authentication authority Web services published by other said gateway authority entities **[*page 3 paragraph 0032, 0034* "The logical interface and the service implementation are described by the Web Services Description L-anguage (WSDL). WSDL is an XML vocabulary used to automate the details involved in communicating between Web services applications, Referring back to FIG. 1, the service can be publicized by being registered in a standard-format web registry 13. This registry makes it possible for other people or applications to find and use the service. For example, one can publish descriptive information, such as taxonomy, ownership, business name, business type and so on, via a registry that adheres to the Uniform Description, Discovery and Integration (UDDI) specification or into some other XML registry"].**

As per claim 4, the rejection of claim 1 is incorporated and further L. Brown teaches:

authentication authority means, said authentication handler means, and said authentication client means are arranged to use Simple Object Access Protocol (SOAP) to communicate, and use Hypertext Transport Protocol (HTTP) packets to transmit data over Secure Socket Layer (SSL) **[*page 3 paragraph 0043* "The SOAP security extension included with WebSphere Application Server 4.0 is intended to be a security architecture based on the SOAP Security specification, and on widely-accepted security technologies such as secure socket layer (SSL). When using HTTP as the transport mechanism, there are different ways to combine HTTP basic authentication, SSL, and SOAP signatures to handle varying needs of security and authentication"].**

As per claim 5, the rejection of claim 4 is incorporated and further L. Brown teaches:

Data contains means to be transmitted by using File Transport Protocol (FTP) and Simple Mail Transport Protocol (SMTP) **[*page 3 paragraph 0031* "it is possible to send SOAP messages over IBM MQSeries®, FTP or even as mail messages"].**

5. Claims 7, 12, 13, 16 and 17 are rejected under 35 USC 103 (a) for being unpatentable over Yu et al (US Patent No. 6,067,621) in view of Vaeth et al (US Patent No. 6,035,402), in view of M. Brown et al (US Patent No. 6,658,415) and further in view of Vandergeest et al (US Pub No. 2002/0169988).

As per claim 7, the rejection of claim 1 is incorporated and further Yu, Vaeth and M. Brown don't teach that authentication authority registers and manages user identity, authentication client identity (i.e. device ID), user private identity (i.e. password), and associated vital information (i.e. biometric information).

However Vandergeest teaches that authentication authority registers and manages user identity, authentication client identity (i.e. device ID), user private identity (i.e. password), and associated vital information (i.e. biometric information) **[Fig. 3 *page 2 paragraph 0019* "the authentication database 18 stores, for a plurality of users, on a per-user basis, a user ID 24, associated password or hashed password 26 (if used) and destination unit data 22. The authentication database 18 may be populated based on a registration process carried out between a user device and the second unit 12" *page 3 paragraph 0020* "the first unit 10 responds by sending the primary authentication information 32, namely, the user ID and password (if required). This may be provided, for example, by a person through an input device, such as a keypad. It may be a biometric input device, may be a hardware token, smart card or other suitable mechanism"].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Vandergeest into the teaching of Yu, Vaeth and M. Brown to use authentication unit and authentication database for registering and managing the user's multi-factor authentication information. The modification would be obvious because one of ordinary skill in the art would be motivated to utilize multi-factor authentication techniques for improving the authentication process as compare to two factor authentication **[Vandergeest, *paragraph 0005, 0006*].**

As per claim 12, the rejection of claim 11 is incorporated and further Yu teaches:

synchronization codes are arranged to be generated by math functions comprising hash, power and modular math operators **[*col. 5 17-21* "The one-time password is generated by the steps of inserting the counter value into a password bit stream produced by performing a one way hash function on the value output through the symmetrical key cipher algorithm"].** Yu doesn't clearly teach the user identity, authentication client identity and user private identity (i.e. password) as the input information.

However Vandergeest teaches the user identity, authentication client identity (i.e. device identity) and user private identity (i.e. password) as the input information ***[page 2 paragraph 0019*** **"the authentication database 18 stores, for a plurality of users, on a per-user basis, a user ID 24, associated password or**

hashed password 26 (if used) and destination unit data 22", paragraph 0016 "an authentication database is maintained which contains per-user destination unit data (i.e. device identity)**, including, for example, a destination unit identifier such as a phone number of a radiotelephone, an IP address, a pager number"].**

As per claim 13, the rejection of claim 12 is incorporated and it encompasses limitations that are similar to limitations of claim 12. Thus, it is rejected with the same rationale applied against claim 12 above.

As per claim 16, the rejection of claim 15 is incorporated and is rejected for the same reason set forth in the rejection of claim 12 above.

As per claim 17, the rejection of claims 7, 12, 13 and 16 are incorporated and further Vandergeest teaches:

user private identity comprises said user's biometric identity and other shared secret information (i.e. password or private key) **[page 3 paragraph 0020 the first unit 10 responds by sending the primary authentication information 32, namely, the user ID and password (if required). This may be provided, for example, by a person through an input device, such as a keypad. It may be a biometric input device** (i.e. biometric input device use for entering the user's biometric information)**].**

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Audebert et al (US Pub No. 2002/0194499) discloses intelligent portable device as credential storage and cryptographic service provider and business transactions terminal.

Sixtus (US Patent No. 5,903,721) discloses that a method for executing a secure online transaction between a vendor computer and a user computer, wherein the vendor computer and the user computer are interconnected to a computer network such as the Internet for data communications therebetween.

Fiammante (US Pub No. 2003/0191721) discloses that a system and a method for associating communication devices like a computing device and a wireless portable device so as to carry out secure transactions over an untrusted network like the Internet.

Crane et al (US Patent No. 6,510,236) discloses that an authentication framework for authenticating clients, each of which is coupled to an authentication device of one of a plurality of permitted authentication device types.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NBP

7/14/05

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135